SOC IMS: SOC-20160131-650075

Last Updated: 2/3/2016 9:04 AM

SOC Incident Management System

IMS User Contact:	(b) (6)	**Restrict Access To:**	All IMS
Record Permissions Group:	All IMS Users	**Record Source:**	

Contact Details

Enter the NASA AUID or email address of the Contact, and click "Lookup Contact Details" to automatically retrieve the information.

AUID:		**Email:**	

Enter Contact information below if the primary contact is not an IMS user

Contact Last Name:		**Contact First Name:**	
Contact Role:	NASA Other	**Contact Office Phone:**	
Contact E-mail:		**Contact Cell Phone:**	
Contact AUID:		**Contact NASA Center:**	
Contact Building:		**Contact Room Number:**	
Contact Type:			

General Details

SOC Tracking Number:	SOC-20160131-650075	**Categorization:**	Incident

Date Record Created (UTC):	1/31/2016 10:01 PM	**Incident Time Zone:**	UTC - Coordinated Universal Time Zone (GMT)
Title:	Potential NASA/AnonSec intrusion		

Brief Description:

Subject: Potential NASA/AnonSec intrusion

Chapters 1-4 of the document largely appear to be a mix of open source information, exaggerations, and old data (see the end of this message for more details)

Chapters 5 and 6 may correspond to a recent but remediated intrusion of NASA systems. It appears AnonSec may have gained (and then lost) access to at least two unclassified/internet-connected systems associated (b) (6), (b) (7)(C) [redacted] (b) (6), (b) (7)(C) [redacted] an (b) (6), (b) (7)(C) [redacted] at NASA's (b) (6), (b) (7)(C), (b) (7)(E) [redacted] associated with the Dryden Flight Research Center.

Specifically, AnonSec claims to have accessed at least two Linux systems associated with (b) (6), (b) (7)(C) [redacted] and three Western Digital NAS drives containing (b) (6), (b) (7)(C) [redacted]. They also (b) (6), (b) (7)(C) [redacted] (b) (6), (b) (7)(C) [redacted] I find that last claim fairly dubious, but not impossible.

It's unclear when this intrusion supposedly occurred. However, searching for the hashtag OpNasaDrones on twitter revealed posts by Anon members appearing to refer to this intrusion dating back to January 2015 or even late 2014. In terms of the end date for the intrusion, AnonSec claims NASA discovered the attack and completely locked them out. Assuming the zine was recently published, this remediation may have also occurred recently. In fact, a tweet one hour ago by OpNasaDrones states "T-Minus 24hrs until #OpNasaDrones leaks & zine released..."

Along with the zine, (b) (7)(E) [redacted] (b) (7)(E) [redacted] I believe the FBI has not yet retrieved the full dataset yet.

Analysis of Chapters 1-4:

(b) (7)(E) [redacted]

- Lines 351-359 (b) (7)(E) [redacted] (b) (7)(E) [redacted] in Chapters 5,6

- From there, (b) (7)(E) [redacted] (b) (7)(E) [redacted]:

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

(b) (7)(E) [redacted] So that's (b) (7)(E) [redacted] (b) (7)(E) [redacted]

- Lines 509-510 are interesting. (b) (7)(E) [redacted] (b) (7)(E) [redacted]

- That takes us to line 547. (b) (7)(E) [redacted] (b) (7)(E) [redacted]

- Lines 925 to 3338 (b) (7)(E)

(b) (7)(E)

.

(b) (7)(E)

(b) (7)(E)

V/r,

(b) (6), (b) (7)(C)

Current Status:	Closed	**Assigned To:**	(b) (7)(E), (b) (7)(C)
Current Priority:	Medium	**Also Notify:**	
CUI:	No SBU or PII	**Notify on Save:**	No
Ok To Close:	Yes		

US CERT Reporting

Risk Rating:			
Information Impact:		**Functional Impact:**	
Recoverability:		**Attack Vectors:**	Web Email/Phishing
Critical Service or System:		**Classified Incident:**	
Major Incident:		**High Value Assets (HVA):**	
Reportable to Congress:			
Observed Activity:		**Number of Records Impacted:**	
Location of Observed Activity:		**Number of Systems Impacted:**	
Actor Characterization:		**Number of Users Impacted:**	
Action Taken to Recover:		**Number of Files Impact**	

		ed:	

The fields below hold the US-CERT Reporting fields that were in force from October 1, 2015 through March 31, 2017. The are included here for reporting purposes only.

Functional Impact old:	None	**Informational Impacts old:**	None
		Recoverability Impact old:	Not Applicable

Related Tasks

Task ID	Assigned To	Due Date (UTC)	Priority	Status	Description	Resolution
No Records Found						

Related Incidents

Select Relationship:		**Relationship Description:**	

Parent Incident

SOC Tracking Number	Current Status	Title
No Records Found		

Child Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Sibling Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Incident Details

Time Incident Started:		**Time Incident Started (UTC):**	
Time Incident Detected:		**Time Incident Detect**	

		ed (UTC):	
Center Affected by Incident:	HQ	Overall Impact (reference):	Low
US-CERT Category:	CAT 6 - Investigations	Incident Subcategory:	
US-CERT Tracking Number:		ESD Ticket #:	
Resolution Status:	Duplicate	Malware Family:	
		Highest level of access gained:	
Primary Method used to Identify Incident:	User		
Primary Attack Category:			
Primary Vulnerability Type:		Lost or Stolen NASA Equipment:	None

Lost or Stolen NASA Equipment Application

Tracking ID	Cause of Loss	Type of System Lost	Description of Circumstances
No Records Found			

Host Information

NASA Hosts

IP Address	IPv6 Address	Host Name	Center/Facility
No Records Found			

External Hosts

IP Address	External IPv6 Address	Host Name	Position in this attack

No Records Found

Campaigns

Campaign Name:		**Reviewed By TVA:**	
Campaign Comment:		**Confirmed By TVA:**	
		Is APT:	

Indicators of Compromise

IOC Domain

FQDN	Do Sinkhole	Comment
No Records Found		

IOC IP

IP Address	IP Block	Comment
No Records Found		

IOC File

Filename	MD5 Hash	Comment
No Records Found		

IOC Registry Key

Key Name	Key Value	Comment
No Records Found		

IOC Email

Sender Email	Subject	Comment
No Records Found		

IOC Detection

Name	Type	Comment
No Records Found		

Root Cause Statement

The Root Cause Statement can be constructed from the following fields like so:
"SOURCES source realized CATEGORIES using METHODS exploiting CAUSES (with additional FACTORS) gaining OBJECTVES."
See the help for the individual fields for more information about what the various values mean and their context.

Root Cause Sources:		**Root Cause Categories:**	
Root Cause Methods:		**Root Cause Causes:**	
Root Cause Factors:		**Root Cause Objectives:**	

Reporting Organizations

Reporting Date (UTC)	Reporting Local Date	Reporting Local Time Zone	Reporting Notes	Reporting Number	Reporting Organization	Reporting Organization Contact
No Records Found						

Impact of Incident

NASA Programs, Projects, and/or Operations:		**People:**	
Data (at Rest or Transmission):		**System:**	
Cost:		**Sophistication / Nature of Attack:**	
Number of systems affected by this incident:		**Number of NASA Centers/ Facilities affected by this incident:**	
Number of accounts affected by this incident:		**Critical Infrastructure Impacted:**	

Other Impacts:	
Overall Impact:	Low -- Incident Considered Low if none of the below Categories are rated Moderate or High

Containment Actions

Incident Containment System Action:	
Incident Containment Network Action:	

Recovery Actions

Incident Recovery System Action:	
Incident Recovery User Action:	

Recommendations

Root Cause:	
Lessons Learned:	

Costs

Center (Hours):		**Center (Dollars):**	
NASA SOC (Hours):	1.00	**NASA SOC (Dollars):**	100.00
NASA NOC (Hours):		**NASA NOC (Dollars):**	
Other Costs (Hours):		**Other Costs (Dollars):**	

Total Costs in Hours and Dollars are automatically calculated as the sum of the individual costs above. Center IR teams or managers should enter the Center costs, the NASA SOC Manager should enter the SOC Costs and the NOC Manager should enter the NOC costs, if any, in order to arrive at the Total Cost.

Total Cost (Hours):	1	**Total Cost (Dollar**	100

		s):	
Description of Costs:			
System Down Time (Days):		System Down Time (Hours):	

Timeline

Date Record Opened (UTC):	1/31/2016 10:01 PM	Date Record Confirmed (UTC):	2/3/2016 5:35 AM
Date Record Contained (UTC):	2/2/2016 4:33 PM	Date Record Resolved (UTC):	2/2/2016 4:33 PM
Date Record Closed (UTC):	2/3/2016 9:04 AM		
Time in Open:	(b) (7)(E)		
Time in Confirmed:	[redacted]	Time to Confirm:	(b) (7)(E)
Time in Contained:	[redacted]	Time to Contain:	[redacted]
Time in Resolved:	[redacted]	Time to Resolve:	[redacted]
Time in Closed:	[redacted]	Time to Close:	[redacted]
Number of Days to Resolve:	[redacted]		

Journal Entries

Entry	Entry Date	IMS User
original investigation done on ticket SOC-20160129-649963, this ticket is being resolved as duplicate to that orginal ticket Please update the original ticket with any additional information SOC-20160129-649963.	2/2/2016 4:15 PM	(b) (6), (b) (7)(C) [redacted]
SOC; Please open an IMS ticket; attached is information reported by the FBI identified through open source below is a summary, the information date is believed to be sometime in Jan 2016. The open source information seem to claim that a compromise happened on (b) (7)(E) [redacted] (possibly used or administrated by (b) (7)(E), (b) (6) [redacted] (b) (7)(E) [redacted] ARC). Subject: Potential NASA/AnonSec intrusion Chapters 1-4 of the document largely appear to be a mix of open source information, exaggerations, and old data (see the end of this message for more details) Chapters 5 and 6 may correspond to a recent but remediated intrusion of NASA systems. It appears AnonSec may have gained (and then lost) access to at least two unclassified/internet-connected systems associated with (b) (6), (b) (7) [redacted] (b) (7)(E), (b) (7)(C) [redacted], an (b) (7)(E) [redacted] (b) (6), (b) (7) [redacted] at NASA's (b) (7)(E), (b) (7)(C), (b) (6) [redacted] utilizes Global Hawk drones associated with the Dryden Flight Research Center. Specifically, AnonSec claims to have accessed at least two Linux systems associated with (b) (7)(E), (b) (7)(C) [redacted] and three Western Digital NAS drives containing (b) (7)(E), (b) (6) [redacted] (b) (7)(E), (b) (6), (b) (7) [redacted] They also (b) (7)(E), (b) (6), (b) (7)(C) [redacted] (b) (7)(E) [redacted] I find that last claim fairly dubious, but not impossible. It's unclear when this intrusion supposedly occurred. However, searching for the hashtag OpNasaDrones on twitter revealed posts by Anon members appearing to refer to this intrusion dating back to January 2015 or even late 2014. In terms of the end date for the intrusion, AnonSec claims NASA discovered the attack and completely locked them out. Assuming the zine was recently published, this remediation may have also occurred recently. In fact, a tweet one hour ago by OpNasaDrones states "T-Minus 24hrs until #OpNasaDrones leaks & zine released..." Along with the zine, (b) (7)(E) [redacted] (b) (7)(E) [redacted] I believe the FBI has not yet retrieved the full dataset yet. -- Analysis of Chapters 1-4: (b) (7)(E) [redacted] - Lines 351-359 (b) (7)(E) [redacted] (b) (7)(E) [redacted] in Chapters 5,6 - From there, (b) (7)(E) [redacted] (b) (7)(E) [redacted]: (b) (7)(E) [redacted]	1/31/2016 9:56 PM	

- (b) (7)(E) [redacted]

[redacted] So that's (b) (7)(E) [redacted]

- Lines 509-510 are interesting. (b) (7)(E) [redacted]

- That takes us to line 547. As far as I can tell, everything from line 547 to line 923 is content they downloaded from various internet websites. I (b) (7)(E) [redacted]

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

V/r,

(b) (6), (b) (7)(C) [redacted]

README (1).txt

```
-----BEGIN PGP SIGNED MESSAGE-----
(b) (7)(E) [redacted]

Version: OpNasaDrones
pub   4096R/4AAE63E0 2015-10-01
      Key fingerprint = DEFD 83DD 81B5 A61D 9959  C009 4CFF 6773 4AAE 63E0
uid                  AnonSec (Nihil Verum Est Omnia Licita)
<An0nsec@protonmail.ch>

         .8.          b.             8     ,o888888o.     b.             8
d888888o.   8 8888888888       ,o888888o.
        .888.         888o.          8  . 8888     `88.   888o.          8
.`8888:' `88. 8 8888            8888     `88.
       :88888.        Y88888o.       8 ,8 8888       `8b  Y88888o.       8
8.`8888.   Y8 8 8888         ,8 8888       `8.
      . `88888.       .`Y888888o.    8 88 8888        `8b .`Y888888o.    8
`8.`8888.     8 8888         88 8888
     .8. `88888.      8o.  `Y888888o. 8 88 8888        88 8o.  `Y888888o. 8
```

~~~
`8.`8888.    8 888888888888 88 8888
    .8`8. `88888.     8`Y8o. `Y88888o8 88 8888         88 8`Y8o. `Y88888o8
`8.`8888.   8 8888         88 8888
   .8' `8. `88888.    8   `Y8o. `Y8888 88 8888        ,8P 8   `Y8o. `Y8888
`8.`8888.  8 8888         88 8888
  .8'   `8. `88888.   8      `Y8o. `Y8 `8 8888       ,8P  8      `Y8o. `Y8 8b
`8.`8888. 8 8888         `8 8888       .8'
 .888888888. `88888.  8         `Y8o.`  ` 8888     ,88'   8         `Y8o.`
`8b.  ;8.`8888 8 8888            8888     ,88'
.8'       `8. `88888. 8            `Yo     `8888888P'     8            `Yo
`Y8888P ,88P' 8 888888888888      `8888888P'

           4c 61 75 67 68 69 6e 67 41 74 59 6f 75 72 53 65 63 75 72 69 74 79 53
69 6e 63 65 32 30 31 32

                                              `                ```
                                      ```  ... ````        ``  ``--` ``
                            ``.  .--.  ..``-.-.`      `..````.:. .-..  ```
                             `  ---```.`.` -..`              `.`-  `..:. ` --`
`
                           .--   `---` ``..                         `...` `.-.`
.--
                   `.``.:.`` `````                                    ...
```.-- `-.
                    ` .--`````.`
....``` --. `
                  ``. ....``` `                ``````.`````-``  ``
`````....` .``
                ` .-.```.```.              ```..---....`.-----``.-.. `
``...```... `
               `.``.`-.```                ..-.`..:`.--..-::.-.`...`-.-`
. .:..-. .`
              .--.`` .-.`              `.--.`-.....---..`----.--`--`---.``
`.-` ``.`-`
            ` `.`.---.`              `-.--...-.-.-...`.-`..--.`...-.-..:...
`.```--.```
           `-.````...               `...`.`.--``-..........-...-.`.......`..
`...`` .`
           `-..`````               ```..```.--...`...--....-`..--..`.-......`
```. `.``
          .``-....``               ..`..  ...----`........--....-..`.---.---.
`.`.``.````
         ..-```..`                `-.-.  ``-....-:.-.``..-..........-....--..
...````-.
        `---..---.                `--`  ./.---..`--......--:---`---.-..-.---.
-::----..
       `. `.`--.                  `:-. `.-..-.`.---:----..-  ---::----..-..-:
`- ..``  ..
       .--```.`.`                 `--` ---.```    `..:...-.-`   ` `--.--..`-.
`:.````.--
       .-....-.``                 `-.. ..-.        ``..`..-`       ``---`.`.`
.--......
      ```...--``                   ..` .`..         `-...:-          --.``..`
....-...``
      ..` ``  .`                   `-. ..-          .-..`--`         .-.``-..
.`   `  `.
       ..`..---.                      `---         .``.-...-`        ..:  .
.--.`..`.-
       ``.`.--`                     ``.`.-`      `-..-. `---.``    `.--.`
.``..``
      .` `` `--.                   ..`.-.------:-`-..-   .--.-..-..`-:----.-
`.`   `-:
      `..`.`.-.`                    .:..-``....--:--.     ......-.--..-.`--.
~~~

~~~
.-.``..`.`
      `.......```                     ```-:.-....`...` `.` .--..`....-..-.
```..`..`.`
        `.`````..                        ..``..``.--.`...``-.`-..--.`.```
--   `````
       ---.``--..                            `....-..-:.-....`-..---`
:-````.:--
       `----::`.` `                      .`   `--.--.....---.-``..
``/-.---.-
          ```. `--.                      ---.    `...-..---..```   ---
---``` ```
         ..-..`.---``                    .-...   .. .``.`.. -`   `-`--
--`.``-...`
         `.-..-...`.-`                   ....-.     `     ` `    .--:`
````.-.--...`
          `.....``  .-`                   ..--`                   `.-..`
`.`.```...```
            ```  ```.```                  ...-.`  ` `  ``  `    `...`.
` `.....` ``
            .--..-.--` --`                 ....-``` ```.`  .`` `-..``
...  `-..``   .`
              `..`  ```.`.` .`              ...--:--.`.....`.......
` `--.``.  .--`
                .......`..` -..               ..`-........-----`-`
..-` --.``.`--.`
                ``..-``.````-`.` ..`            `.--....`.-``-`           ``.
`...`````.....``
                  ``````````...` ...  `  `         ````````  `       ```  ``...
``..``` ``````
                      ..````-..` `..`. ..``                      ``.--`.---.
`.``--.-`
                      .``.-.`  ```--:. ..`-.                     -..-`
.:-.```  `.--`.`
                            `.:- .--`` `-.-.                     `-.````.-..
.-.`
                            ``-`--.  `..-..` ````           ```.``-.`..`
.`-::-`
                                ```-..---``    `   ``````   `    ``.--..`.`
~~~
                                  `````..`   `` `          ``.`` ``
                                                   #AnonSec
                                          /dev/null before dishonour

+   o   +   o
  BEWARE   +------------------------------------+
+   o   +   +
                                  OF | Table of
Contents | o   +
             RANTS,
|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~| o +   +   +
                                                            | 0x00 -
Preface | +   o   o   +   o
                                 RICKTROLLING | 0x01 - FLASH FROM
THE PAST | -_-_-_-_-_-_-_,------,   o
                                                   | 0x02 -
TTP(Tech/Tac/Pro) | _-_-_-_-_-_-_-| /_/\
                            AND | 0x03 - NASA
Missions&Aircraft | -_-_-_-_-_-_-_-~|__(^ .^) +   +
                                                       | 0x04 -
Chemtrails/CS/GE/WM | _-_-_-_-_-_-_-"" ""
```

```
   ROOTKITS                          |     0x05 -  WHATS A ROOTKIT?       |
+         o         +       +
                                     |     0x06 -  Russian Roulette       |
+      o         o   +       o
                                     |     0x07 -  Epilogue               |
+         +

+------------------------------------+     o        o         o      o     +
```

0x00 - Preface

> "Look, the people you are after are the people you depend on. We cook your meals, we haul your trash, we connect your calls, we drive your ambulances. We guard you while you sleep. DO NOT... FUCK WITH US."

Well here we are, its 2015/2016 and shit has gotten weird... like "No more secrets Marty" weird.
But if there is one thing our team has learned over the past years, its that no one has
impermeable OpSec, not even the NSA or GCHQ, e.g. Snowden leaks, ICWATCH, NSA Playset, etc...

Basically, people will ALWAYS be the biggest vulnerability in any networked system.
With that being said, we want to take the time to thank all baby boomer secretaries world-wide, without your lack of training and irresistible urge to open attachments in
spoofed emails from the HR department, this would have never happened lol // Gozi ftw ?? ,,???,, ??

```
+==================================================================================+
```

```
                                .-------.
                     .'         `.
                   .'             `.
                   |    NO SKIDS   |
                   |    ALLOWED    |
                   |     BEYOND    |
                   '      THIS     '
                    `.   POINT   .'
                      `._______.'   __   __
                          | | .----/  \ /  \---.
                          | | |   |    |    |  |____
                          | | |   |`--''`--'| /  |  \_
                        ,----.|   \~O~| ~O~ _ |  |  | \
                        | ---'|    '._/ \_.| `|  |  | |
                        \.---'|            |  | `- ,| |
                         `---'|            | :        |
                          | | |            |  '._.--  ;
                          | | |    .      .:      `  /
                          '-' |     '....'  `.______/
                              |                |
                              |                |
                              `----------------'
                                 ||       ||
                                 ||       ||
                            _.---''`  '-,  ,-'  ''---._
                           /        __..'   '..__        \
                           '---''`              `''---'


For those who dont know us, AnonSec was created in Nov 2011 by MrLele(a former
AnonGhost admin,
now Peshmerga sniper) and AnonSec666(US python programmer). Since our start with
two members from
Kurdistan and USA; we have come a long way; adding members and associates from
the UK, Germany,
Japan, Malaysia, Morocco, Indonesia, India, Pakistan, Iraq, Italy, Romania and
even Latvia.  //shouts to CWA, LizardSquad & TeaMp0isoN || rip alg0d
Here are just a few Operations we either started or were heavily involved in...
```

(b) (7)(E)
[redacted]

```
     -
https://www.cyberguerrilla.org/blog/anonymous-operation-nasa-drones-anonsec/
     - http://cyberwarzone.com/anonsec-hackers-claim-hacked-nasa-drones/
==> #OpBeast/OpNullDenmark == after DDoSing, defacing or rm -rf / 100's of
beastiality sites, Denmark finally changed their laws
     -
http://www.mirror.co.uk/news/technology-science/technology/anti-bestiality-ha
ckers-target-vile-dog-5310038
     -
http://www.techworm.net/2015/04/anonymous-launch-opbeast-against-animal-cruel
ty-and-depravity.html
     -
http://www.bbc.co.uk/newsbeat/article/32411241/denmark-passes-law-to-ban-best
iality
==> #OpDetroit             == DDoS servers over Detroit water shutoffs also
seized a Detroit govt DB and demanded BTC ransom
     - http://www.rt.com/usa/206663-detroit-bitcoin-ransom-database/   // they
never mentioned AnonSec even tho a member was v& over it *sigh*
     -
http://www.techworm.net/2014/11/hackers-encrypted-entire-city-detroit-databas
e-demanded-ransom-2000-bitcoins-803500.html
          - http://pastebin.com/raw.php?i=fc5s029B
          -
http://www.usatoday.com/story/news/nation/2014/08/04/detroit-water-shutoffs/1
3584027/  // Detroit suspended water shutoffs until August 25th, 1 day after we
demanded
==> #OpIsrael              == once a year we join in the chaos of fucking raping
Israeli cyberspace in protest of the current apartheid #FreePalestine
     - https://en.wikipedia.org/wiki/OpIsrael
          - https://www.rt.com/news/opisrael-anonymous-final-warning-448/
          - https://www.rt.com/news/anonymous-israel-cyber-attack-737/
     - https://www.youtube.com/watch?v=Uxy57ofajwE
     - https://www.youtube.com/watch?v=usk0cl0OHwY
          -
https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/anonsec-allegedly-
hacks-israel-defense-forces-military-preparatory-school-in-support-of-palesti
ne.html
==> #OpISIS/#OpTerror4ISIS == worked with GhostSec to take down thousands of ISIS
twitter accs, websites and forums
     -
http://www.techworm.net/2015/04/opisis-anonymous-release-list-of-70-pro-isis-
```

```
websites-and-14000-of-twitter-ids.html
         - http://cyberwarzone.com/anonsec-declares-war-isis-opterror4isis/
         -
https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/site-1-20-15-anons
ec-announces-operation-terror-4-isis-releases-terrorist-group-government-targ
et-list.html
==> #OpDeathEaters         == Expose a UK Paedophilia network being protected by
the political elite
     -
http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11363303/Anonymous
-hackers-turn-fire-on-global-paedophile-menace.html
     -
http://www.dailydot.com/politics/operation-death-eaters-opdeatheaters-anonymo
us-pedosadism-prince-andrew/
     -
http://www.ibtimes.co.uk/opdeatheaters-anonymous-marches-planned-across-uk-us
-highlight-global-network-child-abusers-1487867
==> After hacking the Windsor University School of Medicine & leaking DBs, we
deleted +$9,000,000 in student loan debt instead of phishing students  ^_^
         -
https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/windsor-university
-school-of-medicine-allegedly-hacked-student-database-leaked.html
         - https://twitter.com/_d3f4ult/status/651290005793472512
==> And tons of others that were rekt for various reasons
     -
https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=sea
rch&task=tag&tagId=658&Itemid=1355
     - https://twitter.com/search?q=%40VaraCyber%20Anonsec&src=typd
         -
http://belsec.skynetblogs.be/archive/2014/11/04/70-000-bitcoin-access-account
s-hacked-at-btc-e-com-and-sold-8318769.html
         -
http://www.bitdefender.com/security/anonsec-hacking-group-breaches-720-random
-sites-worldwide;-mocks-lax-security.html
     -
http://thecryptosphere.com/2014/10/08/anonsec-hackers-tangodown-turkish-e-com
merce-sites/
     - http://www.eduicon.com/News/Details/3485.html
     - http://www.tech.com.pk/2014/01/720-websites-hacked-and-defaced-by.html
     -
http://www.meethackers.com/2014/04/mcdonalds-id-leaked-by-anonsec-hackers.htm
l
     - http://pastebin.com/qYUeCzNJ
     -
http://pancasilacyberteam.blogspot.sg/2014/04/1381-email-dibocorkan-oleh-anon
sec-dan.html
         -
http://www.wired.com/2015/11/cia-email-hackers-return-with-major-law-enforcem
ent-breach/
         - http://zone-h.org/archive/notifier=AnonSec



Since our inception we have certainly had our 'ups&downs' as you could say, from
a core member
getting v&, @MrLele1337 going afk to fight ISIS irl and some even becoming
whitehats at tech
companies(Pr3dat0r). However, we are still here laughing at 'security', exposing
feds online
& fucking everyones databases... long dick style  (•_•) ( •_•)>¬¦-¦ (¬¦_¦)
On a more serious note, this is AnonSec's very first zine!
So grab some popcorn and lets get this blood orgy started...
```

```
             ____________________________________________________
            /                                                    \
           |    _____________________________________________     |
           |   |                                             |    |
           |   |                                             |    |
           |   | root@onion.land:~# irssi                    |    |
           |   |                                             |    |
           |   |                                             |    |
           |   |                                             |    |
           |   |                                             |    |
           |   |                                             |    |
           |   |                                             |    |
           |   |                                             |    |
           |   |                                             |    |
           |   |                                             |    |
           |   |_____________________________________________|    |
           |                                                      |
            \_____________________________________________________/
                   \_______________________________________/
                _______________________________________________
             _-'    .-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.  ---  `-_
          _-'.-.-. .-----.-.-.-.-.-.-.-.-.-.-.-.-.-.-.--.  .-.-.`-_
       _-'.-.-.-. .---.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-`__`. .-.-.-.`-_
    _-'.-.-.-.-. .-----.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-----. .-.-.-.-.`-_
 _-'.-.-.-.-.-. .---.-. .-----------------------------. .-.---. .---.-.-.-.`-_
:-----------------------------------------------------------------------------
-:
`---._.-----------------------------------------------------------------._.---
-'
```

```
+=============================================================================
======+

|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~|
 |~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~NEXT
CHAPTER~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~|

|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~|

+=============================================================================
======+
```

```
      0x01 - FLASH FROM THE PAST
```

Lets take time to appreciate how this all started 2 years ago...

```
 ° ? ? ¸. ¸  ?  :.  . • ? ° ?  .    . .  ¸ .    °  ¸. * ? ¸ .
  ...Long ago   ° ? °  ¸. ? ¸ .  ? ° :.  . • °   .   * :.
 • ? ° ?.in an IRC far, ? ¸     ° ? °?  . * ¸.   ? ? ° . .
 .    . ? °?  . * ? far away.......° ? ? °? ¸ .    °  ¸. * ?
 .   ? ° :.  . • ? ° ?. .  ¸ .  ? ? ° . .  ? °?.   °  ¸.
```

```
$# /join #64616e74657320696e6665726e6f 4c696d626f
(3:24) == Shimo7even [root@onion.land] has joined #64616e74657320696e6665726e6f
(3:24) -REDACTED- : Finally....
(3:24) * -REDACTED- glares at Shimo7even for being late
(3:25) Shimo7even : br00te told me DA willing to sell access?
(3:25) ?? : yes, NASA still
(3:26) -REDACTED- : Nothing interesting on this server but it would serve as a
good foothold in the network
(3:27) Shimo7even : im listening
(3:27) ?? : we held several nets for Miami before v&
(3:27) ?? : we injected our own malware
(3:28) -REDACTED- : pareizs
(3:29) ?? : we have no idea who else they gave access to
(3:29) ?? : did +10,000 bot kills just to be safe
(3:29) pangeran : hhhhhhhhhhhhh itu lucu XD XD
(3:30) Bashtien : so how much you guys want?
(3:30) ?? : -REDACTED-
(3:31) -REDACTED- : So, still think you can afford our services?
(3:31) pangeran : ^^^^^^ hhhhhhhhhhhhhhhhhh ^^^^^
(3:31) Shimo7even : Afford? That's rich
(3:32) Shimo7even : LoLing@You -REDACTED-
(3:33) Sh1n0d4 : play nice..
(3:34) Bashtien : -REDACTED- we have been sitting on a ton BTC-E accs for a while
now..
(3:34) Bashtien : so crypto funds are no problem m8
(3:35) ??? : ^^
(3:35) d3f4ult : We will even tumble the coins multiple times, so they are 100%
clean
(3:35) TGab : Those poor Cossaks, ha
(3:37) Shimo7even : BTC or LTC?
(3:37) ?? : btc
(3:38) ?? : https://anonfiles.com/file/-REDACTED-REDACTED-REDACTED-REDACTED-
(3:39) Bashtien : cant read the url in the screenshot..
(3:41) -REDACTED- : thats a decoy.. open it in a hex editor, there is a url to
a zip containing a txt file with the real backdoor url
(3:41) Sh1n0d4 : that OpSec though lol
(3:43) * TGab crunches popcorn
(3:45) Bashtien : pass?
(3:45) ?? : 547265616368657279 for both the zip and shell
(3:46) d3f4ult : fuhosin ^_^
(3:49) * Bastien starts a slow clap
(3:50) * TGab drops popcorn all over the floor
(3:50) d3f4ult : Awww, was hoping it was rooted
(3:50) -REDACTED- : No but we fingerprinted many outdated systems in the network
(3:51) pangeran : wkwkwkwkwkwkw!!! DA ftw \(^_^)/
(3:51) Sh1n0d4 : well thats good enough for me, wbu shimo?
(3:53) Shimo7even : !sendbtc -REDACTED- -REDACTED-REDACTED-REDACTED-REDACTED-
(3:53) Sh1n0d4 : Well thats a yes haha
(3:53) == ???? [~????@co.in] has joined #64616e74657320696e6665726e6f
(3:53) ???? :
https://blockchain.info/address/-REDACTED-REDACTED-REDACTED-REDACTED-
(3:54) ???? : ??
(3:55) == ???? [~????@co.in] has quit [Client Quit]
(3:55) -REDACTED- : Pleasure doing business, until next time.
(3:55) ?? : ??
(3:56) == ?? [?@58.87.127.147] has quit [Client Quit]


[>Disclaimer: Certain information was -REDACTED- due to privacy concerns or by
request.]
```

```
+=============================================================================
======+

|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~|
     |~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~NEXT
CHAPTER~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~|

|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~|

+=============================================================================
======+
```

~~~==+ THE WORLD IS CORRUPT, DONT BE SHEEP TO THE SLAUGHTER +==~~~
SURVIVE | CONTEMPLATE | INNOVATE

0x02 - TTP(Techniques, Tactics & Procedures)

So yeah, we know what you're thinking, hacking NASA? How fucking cliche...
If only I had a Dogecoin for everytime someone claimed that, amiright?
Its like the boy who cried wolf but with hacking NASA instead lol
But you might be surprised how low govt security standards can be, especially with a limited
budget and clueless boomers controlling the network. NASA has been breached more times than
most people can honestly remember (our favorites were Gary McKinnon && Mendax's milw0rm)
// you know, when people used to have legit reasons for their hacks^^
Reasons from searching for hidden evidence of UFO technology to protesting use of Uranium based rocket fuel ^_^

"What the Fuck gives you freedom,
freedom brings opportunity,
opportunity makes your future"

(b) (7)(E)

[redacted]

Since our first shell in NASA systems just had user acc priv, we were fairly limited as to not only what
~~~

dirs we could access, the commands we could run and the other machine/devices on the network that should have been visible. Getting root access on this box would be ideal, so that what we went for.

Unfortunately, this box was running the latest version of debian and didnt have any local root CVEs(publicly)
and we failed to spear phish the root passwd... luckily MA saved the day with his 2014 bypasses & symlink exploits.
With this we were able to simulate root in a new linux directory and run any command. This allowed us to move tools/utils/modules
(get-pip.py/eggs)/0days to the box as needed[see scp_tools.txt]. scp_tools.txt contains a list of some TTP that were
used to accomplish these hacks, its best to make a couple shell scripts for much quicker downloads(scp_tools.sh).

```
     cat scp_tools.txt

~ Map Network ~
nast -m
reverse-ip lookups
whois & reverse-whois
dirbuster
[MapNet]

~ Scan Ports/Fingerprint/Enumerate ~
unicornscan && onetwopunch.sh
Nmap NSE - NFS - SMB
LinEnum.sh
linuxprivchecker.py
fierce.pl
Bluto
dnswalk
Network Miner

~ Vuln Scanner ~
Linux_Exploit_Suggester.pl
unix-privesc-check
nikto.pl
wpscan.rb
joomscan.pl
uniscan
wapiti
w3af
nipper

~ Bruteforce ~
hydra w/ passwd lists

~ 0days ~
Mauritania Attackers 2014 bypasses & r00t Symlink Exploits
CVE-2013-5065
CVE-2014-0038
WD My Book World Edition SSH root remote enable

~ Packet Capture/Sniffers/Recovery ~
wireshark
tcpdump
dsniff
mimikatz
egrep
```

// special thanks to Mauritania Attacker for his bypasses & symlink exploit ^_^

"Assume every network you're on is malicious"
- Samy Kamar

*Mapping a network can be accomplished a million different ways, depending on the type of box your foothold is.
By that we mean; what OS is it, what utils and dependencies does it have already installed, what privileges do
you have, is there any IP restrictions? Once we had a symlinked r00t directory filled with tools is when the
real fun began... we started mapping their network.

```
 +==========================================================================+
 | Our General Steps for Mapping & Propagating Laterally Through a Network |
 +==========================================================================+
```

1) Once we had access to a box in the network..
[MapNet] Here are just a few simple commands to scan active nodes within a network:

```
arp
nast -m
ip neigh
AngryIpScanner (has GUI)
arp-scan -l -I eth0
ping -b (b) (7)(E)
smbtree -NS 2>/dev/null
nbtscan 1(b) (7)(E)
fping -a -g (b) (7)(E)  2> /dev/null
nmap -sP (b) (7)(E) or nmap -sn 192.168.1.0/24
for ip in $(seq 1 254); do ping -c 1 (b) (7)(E) ip>/dev/null; [ $? -eq 0 ] && echo
"(b) (7)(E) .$ip UP" || : ; done
```

2) Next to get a broader view of their entire network, we started probing whois and reverse-whois lookups on the ip
addresses and domain names we found, as well as registrars info(ex. "222 S Mill Avenue" inurl:domaintools). Also
running Bluto & fierce.pl to find ip leaks via DNS zone transfers. If scans are fruitful with new hosts found, repeat
steps 1&2 on the new addresses. Do this until you cant find any more hosts.

3) Once we started seeing other connected nodes on the same LAN, it was time to run some port scans and do some
passive OS/BIOS fingerprinting. (unicornscan && onetwopunch.sh or nmap NSE scripts come in handy here)

4) After mapping some nodes, scanning ports and fingerprinting; we started looking up CVE's for the different versions
of operating systems and the various services
running.(Linux_Exploit_Suggester.pl, unix-privesc-check, nikto.pl,
uniscan and CobaltStrike are the best for automating this process)

5) Any system running RDP/VNC/SSH/MYSQL should always be bruteforced because its common for administrators to either

leave the default login or to use an extremely common passwd.

(b) (7)(E)

6)* If the site is being used as a public server or for any type of database storage, it will most likely have a CMS(content management system) with a cpanel. So try running cmsmap.py, wpscan.rb or joomscan.pl.

7)* If the server has any kind of web application on it, try running wapiti and w3af.

8)* If there are any firewalls, switches or routers found in the network, try running nipper(SonicWALL lol).

9) Scanners are great for those of us who are either busy or lazy, but they also tend to generate alot of false positive results. One of the most important steps is to use something like dirbuster and manually browse various .xml, .js, .php and php.in files source for SQLi,
XSS, LFI, RFI, FPD, HostHeaderAttacks etc[this requires decent programming and exploitation knowledge to spot possible configuration errors,insecure functions or unsanitized inputs i.e _SERVER["HTTP_HOST"]], unserialize(), popen() , strcmp(), exec(), system(), shell_exec(), escapeshellcmd(), passthru(), create_function(), pcntl_exec(), eval() & many many more!

(b) (7)(E)

(b) (7)(E)

11) Always target the most vulnerable nodes first(minus false positives). //They have many WinXP & unpatched Ubuntu servers btw

- WinXP Local SYSTEM privilege escalation: CVE-2013-5065
- Ubuntu Local root exploit: CVE-2014-0038

(b) (7)(E)

```
                                  \!/ ALWaYS RUN SC4NS oN N3W BOXes FOR MORE NoDES
\!/
```

(b) (7)(E)

15) After a few weeks of repeating this process over&over again on every new box as much as possible, we realized that NASA had many subnets connected in various ways, creating their own supernet.

(b) (7)(E)

```
+=============================================================================
======+

|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~|
     |~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~NEXT
CHAPTER~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~|

|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~|

+=============================================================================
======+
```

"I am not an Athenian or a Greek but a citizen of the world."
- Diogenes of Sinope

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

(b) (7)(E)

[redacted]

~~SENSITIVE BUT UNCLASSIFIED~~

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

While we know some of the data from the missions is supposed to be made public(like majority of NASA missions)
but we inherently dont trust anyone, especially government agencies. So we wanted access to the raw data, straight
from the backend servers, to see if they were not publishing some of the data or possibly tampering with the data
to cover up results e.g. Processed/Unprocessed or Filtered/Raw folders.
(^^just like Ms Donna Hare told Gary McKinnon about Building 8 of Johnson Space Center)
(^^former Aerospace Contractor for NASA who worked on lunar mapping w/ Top Secret Clearance)

"Hackers, we inherently trust no one, including each other."

```
+============================================================================
======+

|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~|
     |~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~NEXT
CHAPTER~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~|

|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~|

+============================================================================
======+
```

0x04 - Chemtrails/CloudSeeding/GeoEngineering/WeatherModification

```
            "What I'm about to tell you is top secret. A conspiracy bigger than
all of us. There's a powerful
            group of people out there that are secretly running the world. I'm
talking about the guys no one
            knows about, the ones that are invisible. The top 1% of the top 1%,
the guys that play God without
            permission. And now I think they're following me."



+========================================================================+
                 | Chemtrails == CloudSeeding == GeoEngineering ==
WeatherModification |

+========================================================================+


One of the main purposes of the Operation was to bring awareness to the reality
of
Chemtrails/CloudSeeding/Geoengineering/WeatherModification, whatever you want
to call it, they all represent
the same thing. (b) (7)(E) [redacted]


ACE     - Aerosol/Cloud/Ecosystem Mission
ATTREX  - Airborne Tropical Tropopause Experiment
DC3     - Deep Convection Clouds & Chemistry
NEXRAD  - Next Generation Weather Radar
SEAC4RS - Studies of Emissions and Atmospheric Composition

There is a distinct difference between a contrail and a chemtrail, and any sane
person should be able to tell
the difference. Contrails, under normal circumstances, dissipate at a constant
rate behind the aircraft while
maintaining the same length. Chemtrails however, do not dissipate at all, instead
they leave streaks across the
sky as far as the eye can see. Not only that but since the aerosols are laden with
heavy metals and  even
radioactive material, so they eventually widen and thin into a haze until the
entire sky is completely covered.
Also note, we are completely aware that under certain weather conditions and
aircrafts flying at certain altitudes
can create a much longer contrail. However it would still dissipate at a constant
rate, not spreadout and cover the
sky without ever dissipating, like Chemtrails.


Chemtrails/CloudSeeding/GeoEngineering/WeatherModification, goes back all the
way to WWII and the Vietnam War.
Here in the video  below is an example the US military creating clouds using planes
exhaust combined with various
chemicals during a Naval exercise. Its said that this was used at sea as a possible
defence mechanism.
https://www.youtube.com/watch?v=rGJvfJUFc9o


+-------------------------------------------------------+
| Former Classified Government Cloud Seeding Projects |
+-------------------------------------------------------+

                 Project Stormfury
```

https://en.wikipedia.org/wiki/Project_Stormfury

Project Popeye(Motorpool/Intermediary-Compatriot)
https://en.wikipedia.org/wiki/Operation_Popeye

Operation Sea-Spray
https://en.wikipedia.org/wiki/Operation_Sea-Spray

If the government has had multiple classified CloudSeeding project in the past, why wouldnt they now? The majority of people find this hard to believe for some reason and will call you crazy. In reality the concept of 'crazy' is completely subjective. One persons saint is another persons sinner, you get what im saying. And a persons perception comes directly from their surroundings, and knowledgebase. Hence, people usually think something is crazy when they havent researched it, i.e. ignorance.

If you arent familiar with this topic, we suggest watching/reading some of the PUBLIC information included in the following links such as wiki's, various patients, diagrams, Pentagon video on targeting religious extremist via air dispersal method(chemtrail) and the documentaries on Chemtrails/CloudSeeding/GeoEngineering/WeatherModification.

Public_Geoengineering_Documentairies_and_Videos.zip
https://mega.nz/#!BQdGAC6J!XWaL3_HRBMbYXBpFa4NHly1nxbTqvY1gyWMJAqi3zSo

Notice how you cant even find the definition of Chemtrail on Wikipedia without being followed by Conspiracy Theory...
However if you read all of the following Wiki's, it becomes apparent that they are all referencing the same process.
https://en.wikipedia.org/wiki/Chemtrail_conspiracy_theory
https://en.wikipedia.org/wiki/Cloud_seeding
https://en.wikipedia.org/wiki/Weather_modification
https://en.wikipedia.org/wiki/Geoengineering
https://en.wikipedia.org/wiki/Climate_engineering

Patients that GeoEngineers reference frequently when talking about Chemtrails/CloudSeeding/GeoEngineering/WeatherModification:
http://prntscr.com/9rl548
http://prntscr.com/9rl5lc
http://prntscr.com/9rl67g
http://prntscr.com/9rl6fu
http://prntscr.com/9rl6ig

Diagrams of GeoEngineers Theory to Block Sun Rays with CloudSeeding & Affect Greenhouse Gases:
http://prntscr.com/9olzrr
http://prntscr.com/9olyvv
http://prntscr.com/9olzio
http://prntscr.com/9olzn1
http://prntscr.com/9olz75

```
+-----------------------------------------------------------------------------
-----------------------------+
|   Chemicals suggested by GeoEngineers for
Chemtrails/CloudSeeding/GeoEngineering/WeatherModification     |
+---------------------------------------------------------------------------
-----------------------------+
 - Aluminum Oxide
 - Barium
 - Strontium
 - Copper Sulfate
 - Potassium Iodide
 - Silver Iodide

MSDS_Aluminum.pdf
https://anonfiles.com/file/55aa2b9d662b59c2e466f139b95ed4c5
MSDS_Barium.pdf
https://anonfiles.com/file/8d483837a4a15f71208b7a28aae5fc03
MSDS_Strontium.pdf
https://anonfiles.com/file/63bfb0194cc6ced8540f58ded175b261


Oxford GeoEngineering
http://www.geoengineering.ox.ac.uk/

Texas CloudSeeding
http://abcnews.go.com/Technology/cloud-seeders-make-rain-drought-stricken-tex
as/story?id=17321980

Texas Weather Modification Bill - H.R. 2995: Weather Modification Research and
Technology Transfer
https://www.opencongress.org/bill/s517-109/show

CIA funds NAS to study GeoEngineering
http://www.slate.com/articles/technology/future_tense/2013/07/cia_funds_nas_s
tudy_into_geoengineering_and_climate_change.html
http://www8.nationalacademies.org/cp/projectview.aspx?key=49540
http://www.nap.edu/catalog/18988/climate-intervention-reflecting-sunlight-to-
cool-earth

China GeoEngineering via CloudSeeding
http://www.news.com.au/technology/chinese-scientists-create-second-artificial
-snowstorm-in-beijing/story-e6frfro0-1225796559341
http://www.telegraph.co.uk/news/worldnews/asia/china/6481650/Chinese-governme
nt-makes-it-snow-in-Beijing-in-order-to-fight-drought.html
http://www.theguardian.com/environment/2009/sep/23/china-cloud-seeding


H.R.2977 -- Space Preservation Act of 2001
http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.2977.IH:

     EXERPT names Chemtrails as Exotic Weapons<

http://prntscr.com/9srrlm



+---------------------------------------------------------------------------
-----------------------------+
| Whistleblowers or Activists publicly against
Chemtrails/CloudSeeding/GeoEngineering/WeatherModification |
+---------------------------------------------------------------------------
-----------------------------+
  - Mark McCandlish: Defence & Aerospace Industry Conceptual Artist &
Designer(former secret clearance)
  - Kristen Meghan: former U.S. Air Force Sr. Industrial Hygienist/Environmental
Specialist
  - Rosalind Peterson: U.S.D.A. certified Farm Service Agency Crop Loss Adjuster
```

- Francis Mangels: U.S.D.A Biologist, Master Gardener soil conservationist
- Ted L. Gunderson: former FBI Head Chief of Memphis and Dallas
- Allan Buckmann: former U.S. Air Force Weather Observer
- Anne K. West: former Army pilot CW2
- Dane Wigington: Solar Expert, Climate Researcher
- Scott Steven: Award Winning Meteorologist
- Dr. Nick Begich: H.A.R.R.P Expert, Author
- Dr. James Fleming: Professor of Science
- Martin Bunzl: Professor
- Dr. Lenny Thyme PhD
- Dr. Tammy L. Born D.O.

...etc...

"The source of information is irrelevant, only its validity."

Related Facts You Need to Know:
1) \!/ Aluminum does NOT exist in nature in free-form, ONLY in compounds \!/
2) Effects of free-form Aluminum Soil contamination causes harsh pH conditions for plant life
http://cru.cahe.wsu.edu/CEPublications/FS050E/FS050E.pdf
3) CDC Reports 1 in 50 American Children Diagnosed with Autism, 10,000% increase
http://www.cdc.gov/ncbddd/autism/data.html
4) Severe increase of Alziehmers and Dementia
http://www.theguardian.com/society/2015/sep/21/one-third-of-people-born-in-2015-will-develop-dementia
5) Bee population decreased 50% due to Aluminum contamination
http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0127665
6) Sub-micron size Aluminum particulates used in CloudSeeding are harmful to human respiration
7) Injecting Aluminum & Sulfate Particles into Stratosphere could have drastic impact on Earths Ozone layer

```
+-----------------------+
| GeoEngineering Quotes |
+-----------------------+
```

"And by the way its not really a moral hazard its more like free riding on our grandkids..."
   - David Keith, GeoEngineer

"Its likely to cause some damage, in some places..."
   - Ken Caldeira, GeoEngineer

"Weather control could become a more important weapon than the atom bomb."
   - U.S. Presidential Advisory Committee of 1957

So if CloudSeeding, GeoEngineering and WeatherModification are all publicly acknowledged as real, why are Chemtrails
discredited when its literally the same exact thing just with a different name?
If you acknowledge that
CloudSeeding/GeoEngineering/WeatherModification is real and know that our government is corrupt and does illegal things
in the dark without congressional approval all the time; then why is the theory of chemtrails so hard to believe?
Everyone knows that the aviation company, Evergreen Air, is a CIA owned asset and is involved in such activities.
Just like 9/11, there are piles of evidence that prove these "Conspiracies" are very real.

The issue of GeoEngineering and Genetically Modified Organisms(GMOs) are extremely interrelated.

Here is a patent titled “Stress tolerant plants and methods thereof,” that is owned by Monsanto, and seems to
address all forms of abiotic stress that weather manipulation and chemtrails can cause:
 Monsanto Drought and Abiotic Resistant Corn
 http://www.google.com/patents/US7851676
"Improvement of abiotic stress tolerance in plants would be an agronomic advantage to growers allowing enhanced growth
and/or germination in cold, drought, flood, heat, UV stress, ozone increases,>>> acid rain, <<< pollution, salt stress,

heavy metals, <<< mineralized soils, and other
abiotic stresses."

Since organic planets(non-GMO) cant grow in harsh environments like GMOs they are forced to use Monsantos seeds. However
they are Terminator Seeds which means they dont reproduce any usable seeds for the farmer, they have to keep buying more.
So no more independent farmers and Monsanto controls a majority of the food supply through the farmers.

GeoEngineering kills normal crops -> Monsanto makes resistant crops -> no more independent farmers, Monsanto owns foodsupply

The government hasnt had to change its mass control method, for centuries...

Hegelian Dialectic

```
                        +---------------------------------------+
                                                   | Problem  =>  Reaction  =>
Solution  |
                             +---------------------------------------+
```

Highly toxic soil environments cant grow organic food so they need GMO seeds which are resistant
but contain toxic chemicals like Glyphosate(which is gene spliced,grafted, into the seeds genetics)
 1 Glyphosate is a known endocrine disruptor.
 2. Endocrine disruptors can cause organ and neurological damage.
 3. Glyphosate damages the mitochondria and its functions
 4. Roundup™ and GMOs have shown liver and kidney damage and abnormal behaviour

in rat studies.
 5. Use of glyphosate on herbicide-resistant crops has skyrocketed since 1995.
 6. Incidence, prevalence and deaths due to these diseases has also skyrocketed since 1995(alzeihmers/autism/demenia).

RoundUp Lobbyist Saying its "safe" to drink Glyphosate
https://www.youtube.com/watch?v=ovKw6YjqSfM

Dullards and normies be like...

```
                           Baa.
                  Yea he conspiracy theorist
                    I hear he smoke weed                 Baa.
 Baa.                 Baa..               Caitlyn Jenner is a beautiful
butterfly
Those are contrails       |                  I love FOXNEWS, such American
You are crazy           |                  / GMOs are delicious!
Baa..                  |                  /    Baa..
 \         __ _       |                  /
  \    .-.'  `; `-._  __  _         __ _
   \  (_,          .-:'  `; `-._.-.:'  `; `-._
    ,'o"(  "SHEEP(_,            (_,             )
   (__,-'      ,'o"(  "SHEEP,'o"(  "SHEEP"    )>
      (       (__,-'       (__,-'              )
       `-'._.--._(             (             )
               |||  |||`-'._.--._.-' `-'._.--._.-'
                               |||  |||      |||  |||
```

We all know these people, the ones who will make up an infinite amount of excuses for any given situation, mostly regurgitated non-sense from our friends at FoxNews lol No amount of scientific evidence or high ranking officials testimonies will change their minds...

We find it staggering how many people still dont believe the federal government is doing this when its already public knowledge that the CIA is funding studies, certain states and countries already have WeatherModification programs in place for the past several years, not to mention all the government whistleblowers. Also other governments are alot more open about their use of weather modification, like China. They admitted to using it during the Olympics as well as trying to make it rain to fight drought, but ended up making a massive snowstorm. (b) (7)(E) [redacted]

At this point if you dont believe in Chemtrails/CloudSeeding/GeoEngineering/WeatherModification, then you are either incapable of using Google, autistic or a paid government disinfo shill (JTRIG).

Most of us in the security field were already aware of this but after the Snowden leaks, it was proven(JTRIG).
https://theintercept.com/2014/02/24/jtrig-manipulation/

Also you must understand the Five Eyes have massive state-sponsored armies of paid disinfo agents

and trolls all over the internet, much like the web brigades.
https://en.wikipedia.org/wiki/Web_brigades

"Condemnation without investigation is the height of ignorance."
– Albert Einstein

As to the exact motive for all this illegal Chemtrails/CloudSeeding/GeoEngineering/WeatherModification, we can only speculate. There are MANY theories, some completely logical while other are a bit of a stretch.

Possible Motives for
Chemtrails/CloudSeeding/GeoEngineering/WeatherModification:
- Solar Radiation Management
- Military Battlefield Dominance
- Complete Population Control
- Control of Food supply via Aluminium Resistant GMO see patients(Monstanto) & Killing Bees
- Profit from Hedged Commodities Insurance; Manipulate Stocks
- Create Economic Instability, food riots from crop failure
- 'Dumb down' populations with hazardous nano particulates of metals
- Depopulation via Massive 'Slow Kill'
- Simulate Biblical Endtimes

...etc...

Sites for monitoring US from satellite imagery:
http://weather.cod.edu/satrad/
http://contrailscience.com/map/
(b) (7)(E) [redacted]

In the end, its honestly sad that we even have to do all this just to prove something so
insanely obvious. Some of our more nihilistic members think that if you cant decipher
the difference between a normal contrail and a chemtrail without a bunch of pdfs, videos,
and web links then you should just put a brown paper bag over your head and lay down...

```
(23:35) Bashtien : Bro, you're wayyy off-topic and ranting again lol
(23:36) * TGab sighs
(23:36) TGab : I know but people need to understand all these issues are connected
(23:36) TGab : Also my rants are all I have left...
(23:37) TGab : Either way, add that shit to the zine but with a warning disclaimer
or something haha
(23:37) Bashtien : Beware of Rants?
(23:38) TGab : Yeah, I like that XD
```

Our ELECTIONS have been replaced with SELECTIONS, thus we must react in order to survive.

The world is not as it seems...

```
+==============================================================================+

|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~|
     |~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~NEXT
CHAPTER~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~|

|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~|

+==============================================================================+
```

0x05 - WHATS A ROOTKIT?

"What is a rootkit?"
"It's like a crazy serial rapist with a very big dick!!"

(b) (7)(E)

Shouts to (b) (6), (b) (7)(C), literally none of this would have been possible without you.. we were stonewalled twice lol

```
                 ___                           (_)
               _/XXX\
_             /XXXXXXX\_                                    __
X\__    __   /X XXXX XX\                           _       /XX\__      ___
    \__/  \_/__        \ \                       _/X\__   /XX XXX\____/XXX\
  \  ___   \/  \_       \ \               ___  _/      \_/  _/   -  __   -  \
 ___/   \__/   \ \__      \\__           /  \_//  _ _ \  \     __  /  \_____/
/  __    \  /     \ \_    _//_\____   __/    //          \___/  \/     __/
```

(b) (7)(E)

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

0x06 - Russian Roulette

- - From here is where it really got interesting.

Basically so far we breached and even rooted many vulnerable NASA systems but what we found next was the most intriguing. From this point in their internal network we could see ALOT more systems and networked devices popping up in scans that were not previously visible before from other machines and external scans.(This means local boxes on their intra network aka ip ranges

(b) (7)(E) [redacted]

Scanning from our most recently rooted Ubuntu system, we fingerprinted yet another identical Ubuntu system, that(praise Cthulu) was vulnerable to CVE-2014-0038 also. It was too easy that most of us thought these might be honeypots lol Luckily for us our tcpdump sniffed some ftp login credentials to the other box that was reused for SSH also(shouts to Jensen, Eric J for continued massive OpSec failure loooooooool).

(b) (7)(E)
^^^Does this look like the face of someone who practices good OpSec? i think not hahahhaha

Once we had user access to the jensen@dryden78 box via SSH is was as simple as wget/src'ing the same CVE-2014-0038 script to the box, compiling and executing(didnt even need to edit the kernel pointers because it was the same exact OS). However this was one of the machines that could only be accessed from within their local NASA network, so we had a couple options of bypassing this for maintained access. Either use one of the squid proxies we setup previously or do some port forwarding magic with socat. If you try to directly access the gateway of this NASA server, you'll be greeted with a message:

(b) (7)(E)

Being the overachiever that Shimo7even is, he did both. Setup a squid proxy on a rooted Ubuntu box as well as configuring socat to portforward SSH connections. Once we rooted this outdated Ubuntu system, we left tcpdump running in the background like usual to sniff plaintext (b) (7)(E). Even setup some SSLstriping, DNSspoof w/ another tcpdump because we noticed some https traffic(port443).

After scanning the network (yet again) from our newest vantage point, we could see several networked storage devices(NAS) with pretty crazy obvious names (b) (7)(E), (b) (7)(E). These turned out to be some (b) (7)(E) to be exact.

[WE KNEW INSTANTLY WE HAD TO HAVE ACCESS TO THESE STORAGE DEVICES ASAP]

However after running a quick portscan on the NAS devices, we noticed only ports 21 & 80 were active(no SSH wtf). Tried both default login combinations on 21&80 but they had been changed... surprisingly. Did some research and found a vulnerability in the firmware update process that allows you to redirect the perl script towards a malicious url and execute arbitrary commands, resulting in an RCE as root 0day(similar to CVE-2013-2251).

(Example) spawn an sshd session by remotely generating ssh keys for root w/o passwd

(b) (7)(E)

(Example) starts the sshd process after each (b) (7)(E)

~~SENSITIVE BUT UNCLASSIFIED~~

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

We repeated this local root via RCE & autostart sshd process on all three NAS devices. However there was some weird error with the exploit that didnt allow us to login to SSH directly as root, so we would have to use a normal user to login and su without a root password.(strange i know) So even though we had basically found a 0day in the WD My Book's to remotely auto-enable sshd as root without a passwd, we still couldnt access the devices, we still needed access to the web portal.

After about one week we checked some of the .csv logs and our SSLstriping+DNSspoof had caught some https logins to some security cams but not the NAS devices. (b) (7)(E) [redacted]

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

"IM DOING MY HAPPY DANCE HAPPY AND ABOUT TO SNORT A LINE RIGHT NOW!!!"

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

...etc

^^^^^

(b) (7)(E)

[redacted]

There were many different ways to move these files out of NASA's network and into our own servers, so we decided to get creative. At first we tried to code some crawlers to scrape all the video and data logs, but we eventually decided to go with another method. Since these storage devices werent even supposed to have SSH installed, massive amounts of port 22 traffic would be suspicious to say the least. (b) (7)(E) [redacted]

(b) (7)(E)

[redacted]

Not sure if it actually helped the traffic stay incognito or actually made it stand out more, it was a highdea for sure. Only problem was the WD NAS devices white light version didnt have cron, so we had to install it(shouts to martybugs).

(b) (7)(E)

[redacted]

Now we had all 3 NAS devices automatically making copies of the logs as they are uploaded from the drones and renaming them to look like semi ordinary index files. (b) (7)(E) [redacted]

(b) (7)(E)

[redacted]

```
                                  ¦¦¦¦¦¦¦+¦¦+      ¦¦¦¦¦¦+ ¦¦+    ¦¦+
¦¦¦¦¦¦+¦¦+  ¦¦+ ¦¦¦¦¦+ ¦¦¦¦¦¦+ ¦¦¦¦¦¦¦¦+
                                  ¦¦+----+¦¦¦     ¦¦+---¦¦+¦¦¦
¦¦¦¦¦+----+¦¦¦  ¦¦¦¦¦+--¦¦+¦¦+--¦¦++--¦¦+--+
                                  ¦¦¦¦¦+  ¦¦¦     ¦¦¦   ¦¦¦¦¦¦ ¦+ ¦¦¦¦¦¦
¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦++   ¦¦¦
                                  ¦¦+--+  ¦¦¦     ¦¦¦   ¦¦¦¦¦¦¦¦¦+¦¦¦¦¦¦
¦¦+--¦¦¦¦¦+--¦¦¦¦¦+--¦¦+   ¦¦¦
                                  ¦¦¦
¦¦¦¦¦¦¦++¦¦¦¦¦¦+++¦¦¦+¦¦¦+++¦¦¦¦¦¦+¦¦¦  ¦¦¦¦¦¦  ¦¦¦¦¦¦  ¦¦¦   ¦¦¦
                                  +-+     +------+ +-----+  +--++--+
+-----++-+  +-++-+  +-++-+  +-+   +-+
```

(b) (7)(E)

[redacted]

(b) (7)(E)

[redacted]

Hats off to @Sh1n0d4 for this idea...

```
(24:47) Sh1n0d4 : time for some R&R muahaha
(24:48) Bashtien : rest & relaxation?
(24:48) Sh1n0d4 : no.. russian roulette
```

(b) (7)(E)

(b) (7)(E)

[redacted]

(b) (7)(E) [redacted]

(b) (7)(E) [redacted]

```
        +--------------------------------------------------------------+
                         |                  So to answer the single most asked
question,          |
                         |
                         | (b) (7)(E) [redacted]
[redacted]  |
        +--------------------------------------------------------------+
```

(b) (7)(E) [redacted]

```
When they came back up several days later, we had completely lost access. Not only
were we no longer receiving rsync backups
over SSH. They also had removed ALL our .php & .aspx backdoors and changed pretty
much every single login credential, from ftp
to http.(to be fair the rsync chain told them which servers to focus their
inspection).
```

(b) (7)(E) [redacted]

[redacted] [redacted]

```
+============================================================================
======+

|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~|
     |~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~NEXT
CHAPTER~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~|

|~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~|

+============================================================================
======+
```

0x07 - Epilogue

People might find this lack of security surprising but its pretty standard from our experience.
Once you get past the main lines of defence, its pretty much smooth sailing propagating through a network
as long as you can maintain access. Too many corporations and governments focus 99% on preventing intruders
instead of having viable solutions once there is a security breach, which is guaranteed to happen.

We would also like to address misconceptions about OpNasaDrones from previous articles. When a member whos
main language is Japanese talks to a reporter who's main language is Punjabi, there is bound to be some miscommunication.
Especially when he misunderstood what the .zip we gave him was. It was more or less 90% public information about
Chemtrail/Geoengineering/CloudSeeding/WeatherModification for him to educate himself better on the topic, you know
since most people think its not real. Only a few files, screenshots and videos were actually part of the leak.
Also the part in the OpNasaDrones about Aliens was misinterpretation using Google Translate. What d3f4ult meant to
say was while doing background research into NASA coverups he found out about supposed accounts of UFOs and
aliens working with the government via Gary McKinnons hack. We didnt find anything related to aliens ourselves
as the video made it sounds like, sorry

Also people tend to forget that we have real lives outside of hacking. Which include working, paying bills, taking
care of family/kids, travelling, etc... its not like AnonSec pays a monthly wage lol Since Wikileaks and The Guardian
never responded to our initial leaks, we had to delay releasing. (b) (7)(E) [redacted]

[redacted]

(b) (7)(E)

[redacted]

(b) (7)(E) [redacted]

```
        +----------------------------------------------------------------------
-----------+
```

(b) (7)(E) [redacted]

```
                                                                      "We are on
the verge of taking down this virtual reality..."
```

Attachment(s)

Name	Size	Type	Upload Date	Down loads
(b) (7)(E) [redacted]	(b) (7)(E) [redacted]	(b) [redacted]	1/31/2016 9:56 PM	(b) [redacted]

History Log

View History Log